Risikomanagement des Universitätsspitals Zürich

Pfaff, Dieter ; Thomet, Ursula

DIETER PFAFF
URSULA THOMET

RISIKOMANAGEMENT DES UNIVERSITÄTS-SPITALS ZÜRICH

Risikoidentifikation und -bewirtschaftung bei unterschiedlichen Instrumenten und Methoden

Das Universitätsspital Zürich basiert sein Risikomanagement auf COSO Enterprise Risk Management (ERM) sowie dem «3-Lines-of-Defence»-Modell. Die Top-Risiken werden von autonomen Risiko- und Kontrollverantwortlichen je nach Objekt und Themengebiet mit verschiedenen, spezifischen Methoden identifiziert und mithilfe eines einheitlichen Risikorasters bewertet und abgestimmt.

1. AUSGANGSLAGE UND ZIELSETZUNG

Das nach Objekten, Themen und Funktionen traditionell sehr unterschiedlich ausgestaltete Risikomanagementsystem des *Universitätsspitals Zürich (USZ)* wurde im Jahr 2013 einer grundlegenden Überprüfung unterzogen. Dabei ging es insbesondere um die Frage einer Vereinheitlichung der bestehenden Konzepte und Instrumente. Das USZ beurteilte den Übergang zu einem integrierten Risikomanagement mit einheitlichen Instrumenten, Vorgehensweisen und Verantwortlichkeiten aufgrund der Breite der verschiedenen Themengebiete und Risiken als nicht zweckmässig. Die verschiedenen autonomen Risiko- und Kontrollinstrumente haben den Vorzug, sich bei der Ausgestaltung des Risikomanagements auf Standards und Rahmenwerke abstützen zu können, die dem jeweiligen Fachthema am besten gerecht werden oder sogar gesetzlich gefordert sind. Auch lassen die spezifischen Instrumente ein Benchmarking mit anderen Institutionen zu. Zudem wurden die Kosten einer Vereinheitlichung (im Vergleich zum beschränkten Nutzen) als zu hoch eingeschätzt. Bereits für den Aufbau eines unternehmensweiten integrierten Risikomanagements wäre mit einem hohen internen und externen Ressourcenbedarf zu rechnen gewesen.

Aus der Überprüfung 2013 ging daher die Zielsetzung hervor, die verschiedenen bestehenden Risiko- und Kontrollinstrumente grundsätzlich zu belassen, sie – soweit zweckmässig – aber enger aufeinander abzustimmen.

Als wichtig wurde angesehen, dass
a) die wesentlichen Risikokategorien und Einzelrisiken mit den vorhandenen autonomen Instrumenten erkannt werden;
b) die Risiken von den verschiedenen Bereichen und Fachexperten beurteilt, bewirtschaftet und rapportiert werden; und
c) die Gesetze und Vorgaben eingehalten werden.

Zudem wurde im Rahmen der Erarbeitung des Konzepts Risikomanagement USZ explizit festgehalten:
1. Die verschiedenen Instrumente sollen miteinander abgestimmt und koordiniert werden; als Grundlage dafür dient die Systematik des Risikomanagements USZ.
2. Unter den verschiedenen Risikomanagement- und Kontrollverantwortlichen soll ein regelmässiger Austausch etabliert werden.
3. Die Top-30-Risiken des USZ sollen aus den verschiedenen Risikomanagement- und Kontrollbereichen in einem einheitlichen Risikoraster mit Eintrittswahrscheinlichkeit und Schadensausmass zusammengeführt und beurteilt werden; die Zusammenführung dient als Basis für die Rapportierung und die Bewirtschaftung.
4. Im Anhang der Jahresrechnung sollen Angaben über die Risikobeurteilung gemacht werden.

Der vorliegende Beitrag gibt einen Überblick über die methodischen Grundlagen des aktuellen Risikomanagementsys-

DIETER PFAFF, PROF. DR. RER. POL., PROFESSOR FÜR ACCOUNTING, UNIVERSITÄT ZÜRICH, ZÜRICH

URSULA THOMET, DIPL. BETRIEBSÖKONOMIN FH, VERANTWORTLICHE INTERNES KONTROLLSYSTEM UND REVISIONEN, UNIVERSITÄTSSPITAL ZÜRICH, ZÜRICH

tems USZ sowie dessen Aufbau und Inhalt. Die Autoren schliessen mit einer Gesamtbeurteilung und einem Ausblick auf Möglichkeiten der Weiterentwicklung (Verbesserung) des Systems.

2. METHODISCHE VORGEHENSWEISE

Das USZ lehnt sich bei der Ausgestaltung des Risikomanagement- und *internen Kontrollsystems (IKS)* grundsätzlich an die international anerkannten COSO-Rahmenwerke an [1]. Die COSO-Rahmenwerke wurden vom Committee of Sponsoring Organizations of the Treadway Commission, einer 1985 gegründeten, freiwilligen privatwirtschaftlichen Organisation entwickelt. Die Organisation hat zum Ziel, Rahmenwerke und Leitlinien für das Risikomanagement, die interne Kontrolle sowie die Betrugsbekämpfung zu entwickeln.

«Die verschiedenen Risikomanagement- und Kontrollinstrumente wenden für den Risikobeurteilungsprozess unterschiedliche Methoden oder Standards an.»

Das Rahmenwerk COSO Internal Control wurde 1992/94 publiziert und im Frühjahr 2013 aufdatiert [2]. COSO ERM für unternehmensweites Risikomanagement wurde 2004 veröffentlicht und stellt eine Ergänzung im Bereich des allgemeinen, unternehmensweiten Risikomanagements dar [3]. Beide Rahmenwerke verfolgen einen risikoorientierten Ansatz. Dies bedeutet, dass Massnahmen und Kontrollen nur dann initiiert werden und damit Kosten verursachen, wenn diese durch ein entsprechendes Risiko gerechtfertigt sind. Der Begriff Risikomanagement versteht sich im USZ im engeren Sinn und betrifft Ereignisse mit negativen Auswirkungen.

Das USZ zieht für die Steuerung, Kontrolle und Überwachung zusätzlich das Modell der «Drei Verteidigungslinien» («Three Lines of Defence») [4] heran, wobei das USZ den Begriff «Linie» anstatt Verteidigungslinie verwendet. Das Modell der drei Linien soll helfen, eine angemessene Governance-Struktur aufzubauen oder aufzuzeigen. Die erste Linie sieht eine Risikosteuerung in den Geschäftsbereichen vor, die zweite Linie wird durch interne Funktionen des Risiko- und Qualitätsmanagements sowie der Compliance wahrgenommen; unabhängige externe Assurance bildet die dritte Linie. Mit dem Konzept der drei Linien wird nicht eine einheitliche methodische Zusammenführung der verschiedenen Risiko- und Kontrollaktivitäten beabsichtigt. Vielmehr zeigt es auf, mit welchen Instrumenten welche Risiken abgefangen werden sollen und wo allenfalls Lücken bestehen.

Die Verknüpfung von COSO ERM mit dem Modell der drei Linien ergibt das «USZ Risk Management» (siehe *Abbildung 1*). Es handelt sich dabei um ein spezifisches Modell, das auf bewährten Ansätzen im Sinne eines Assurance-Konzepts aufbaut. Ein umfassendes Framework als Top-down-Ansatz erleichtert das Verständnis und den systematischen Aufbau eines Risikomanagementsystems. Es bietet die Möglichkeit, effizient Schwächen zu identifizieren und zu beseitigen. Zudem ist es Ausgangspunkt für eine Abstimmung der Teilsysteme. Rahmenkonzepte bieten häufig eine integrierte Sichtweise, welche die Aufdeckung und das Verständnis von Interdependenzen erleichtert. Die an den entsprechenden Prozessen und Elementen beteiligten Mitarbeitenden wie auch die verantwortlichen Organe finden sich rasch zurecht und behalten den Überblick [5].

3. ZIELKATEGORIEN UND RISIKOBEURTEILUNG

Abbildung 1 zeigt, dass aus dem COSO-ERM-Modell die Zielkategorien leicht adaptiert, aber vollständig übernommen werden (Strategie und Kommunikation; laufender Betrieb und Kerngeschäft; finanzielle Führung und Reporting; Gesetze und Regulierung). Für jede Kategorie werden die Grundlagen für die Beurteilung der entsprechenden Risiken festgehalten. Die Grundlagen umfassen neben festgelegten Zielen auch Standards und Benchmarks.

Die verschiedenen Risikomanagement- und Kontrollinstrumente wenden für den Risikobeurteilungsprozess unterschiedliche Methoden oder Standards an. Die Instrumente und zugrunde liegenden Methoden werden den drei Linien nach in einem gemeinsamen Dokument beschrieben und mindestens jährlich aktualisiert.

Beispielsweise setzt das klinische Risikomanagement verschiedene proaktive und reaktive Instrumente und Methoden zur Risikoidentifikation und Beurteilung ein, wie z. B. interne Audits, Schadenfallanalysen, Analysen kritischer Ereignisse aus dem Lern- und Berichtssystem (CIRS USZ) sowie weiterer Meldesysteme. Währenddessen besteht das IKS klassisch aus einer Risikobeurteilung, die auf der Identifikation der finanziell quantitativ und qualitativ wesentlichen Rechnungslegungspositionen und den daraus abgeleiteten Prozessen basiert.

Andere Risikomanagement- und Kontrollinstrumente wiederum – wie zum Beispiel Unternehmenssicherheit, Qualitätsmanagement Forschung und Lehre sowie Datensicherheit und IT-Sicherheit – orientieren sich methodisch an den ISO-Standards.

Abbildung 1 zeigt, dass jede Komponente (A) bis (D) – Risikobeurteilung, Steuerung/Kontrolle (Management Controls), Überwachung (Risk Controls), Überprüfung (Assurance) – für die Zielerreichung aller vier Zielkategorien von Bedeutung ist. Beispielsweise muss im Rahmen eines funktionierenden Risikomanagementsystems sichergestellt werden, dass alle Mitarbeitenden über das für ihre jeweiligen Aufgaben notwendige Fachwissen hinsichtlich Strategie, Prozesse, Berichterstattung sowie der relevanten Gesetze und Normen verfügen. Insoweit kann auch von einer integrierten Sichtweise des Risikomanagements USZ gesprochen werden. Die in den Funktionen und Themengebieten jeweils eingesetzten Risikoinstrumente sind jedoch unterschiedlich.

4. STEUERUNG UND KONTROLLE (MANAGEMENT CONTROLS)

Der *ersten Linie des USZ Risk Management* (Abbildung 1, Buchstabe B) sind die unterschiedlichen Instrumente zugeord-

Abbildung 1: **ÜBERSICHT USZ RISK MANAGEMENT**

A) Risikobeurteilung	Zielkategorien gemäss COSO	Grundlagen zur Risikobeurteilung (nicht abschliessend)	B) Steuerung/Kontrolle Management Controls	1. Linie	Zuständigkeit	C) Überwachung Risk Controls	2. Linie	Zuständigkeit	D) Überprüfung Assurance	3. Linie	Zuständigkeit
Strategie und Kommunikation	↑ Strategie/ Strategieumsetzung ↑ Reputation/ Kommunikation ↑ Margenstärke/ Liquidität/ Vermögen	↑ Entwicklung Umfeld ↑ Erfolgsfaktoren ↑ Strategische Ziele und Absichten ↑ Jahresziele und Vorgaben			Spitaldirektion/ Spitalrat			Strategie-review			
					Prozessverantwortliche/ Verantwortliche IKS			Internes Kontrollsystem (IKS)			
Laufender Betrieb/ Kerngeschäft	↑ Patienten-, Besucher- und Mitarbeitersicherheit ↑ Versorgungssicherheit ↑ Datensicherheit ↑ Geräte und Infrastruktur-sicherheit ↑ Gebäudesicherheit ↑ Sicherheit Bauprojekte ↑ Sicherheit Forschung und Lehre	↑ Benchmark ↑ Standards ↑ Beinahevorfälle ↑ Vorfälle/Ereignisse ↑ Meldungen			Qualität, ärztliche Direktion, Direktion Pflege			Klinisches Risikomanagement			
					Direktion Immobilien			Risikomanagement Gebäude und Bauprojekte			
					Direktion Betrieb			Risikomanagement Geräte und Infrastruktur			
					Direktion Betrieb			Unternehmens-sicherheit			
					Direktion Forschung und Lehre			Qualitätsmanage-ment Forschung und Lehre			
					Direktion Finanzen			Finanz- und Leistungscontrolling			
Finanzielle Führung/Reporting	↑ Verlässlichkeit finanzielle und betriebliche Berichterstattung ↑ Betriebliche und finanzielle Berichterstattung ↑ Finanzielle Sicherheit	↑ Vermögen ↑ Ergebnis ↑ Kostenarten, -stellen und -träger ↑ Budget, Vorjahr ↑ Geldfluss ↑ Kennzahlen			Spitaldirektion			Rechtsdienst			
					Spitalrat			Legal Compliance			
					Datenschutzkommission			Datenschutz			
					Direktion ICT			Datensicherheit und IT-Sicherheit			
					Versicherung			Versicherung und Depot	Schadensabwicklung		
					Operational Audit			Internal/Operational Audit			
Gesetze und Regulierung	↑ Gesetzliche und regulatorische Vorgaben	↑ Gesetze ↑ Regulatorische Vorgaben ↑ Beschlüsse ↑ Meldungen ↑ Beschwerden			Gesundheitsdirektion			Kodier-revision			
					Finanzkontrolle Kanton Zürich			Gesetzliche Revision			
					Diverse externe Revisionen			Leistungsrevisionen, Diverse			
E) Information und Kommunikation											

net, die primär die Steuerung und Kontrolle der definierten Ziele und der täglichen operativen Abläufe zur Aufgabe haben.

So «verstecken» sich hinter dem klinischen Risikomanagement Richtlinien und Handlungsempfehlungen sowie Checklisten und das Vier-Augen-Prinzip als gute Beispiele von Steuerung und Kontrolle.

Typische Massnahmen des IKS sind präventive oder detektive manuelle und automatische Kontrollaktivitäten in den finanzrelevanten Prozessen wie z. B. Prüfung und Genehmigung von Ausgaben im Vier-Augen-Prinzip, Prüfung und Abstimmung von Mutationen.

5. ÜBERWACHUNG (RISK CONTROLS)

Der *zweiten Linie des USZ Risk Management* (Abbildung 1, Buchstabe C) sind die Instrumente des Risiko- und Qualitätsmanagements sowie der Compliance zugeordnet, die innerhalb des USZ eine Überwachungsfunktion wahrnehmen. Sie haben zum Ziel, die Einhaltung der Vorgaben der ersten Linie zu überwachen. Eine Überlappung mit den Aufgaben der ersten Linie ergibt sich insoweit, als die Überwachung zusätzlich die erste Linie bei der Definition von möglichen Steuerungs- und Kontrollaktivitäten unterstützt.

So überwachen beispielsweise die Instrumente Rechtsdienst und Legal Compliance die Einhaltung von rechtlichen Vorgaben der ersten Linie. Zusätzlich unterstützen sie die erste Linie klassisch bei rechtlichen Fragen.

Ein ähnlicher Aufbau zeigt sich beim IKS. Die Überwachung der Umsetzung des IKS und die Bearbeitung von Schwachstellen setzen sich aus unterschiedlichen Elementen zusammen. Soweit möglich und sinnvoll wurden bei der Entwicklung des IKS sogenannte Überwachungs- oder Monitoringkontrollen definiert. Diese Kontrollen sind direkt festgehalten und von den eingesetzten Prozessverantwortlichen durchzuführen.

Auch in den Operational Audits wird die Überwachung des IKS angemessen berücksichtigt. Die Verantwortliche für IKS und Revisionen führt zudem in ausgewählten Bereichen zusätzlich Stichproben und Auswertungen durch. Dies kann risikobasiert oder aufgrund von Hinweisen und Verdachtsfällen sein.

6. ÜBERPRÜFUNG (ASSURANCE)

Der *dritten Linie des USZ Risk Management* (Abbildung 1, Buchstabe D) sind die unabhängigen externen Organe zugeordnet, die eine Überprüfungs- oder Revisionsfunktion haben. Dies sind z. B. die Finanzkontrolle des Kantons Zürich für die Prüfung der Rechnung, die Gesundheitsdirektion des Kantons Zürich für die Kodierrevision sowie diverse weitere Prüfer für gesetzlich vorgegebene Prüfthemen.

Die identifizierten Schwachstellen aus den durchgeführten Prüfungen der Operational Audits (Überwachung oder Risk Controls) und den Prüfungen der Finanzkontrolle des Kantons Zürich (Überprüfung oder Assurance) werden im Massnahmeninventar zentral bei der Verantwortlichen für IKS und Revisionen zusammengetragen und dokumentiert. Die Umsetzung der definierten Massnahmen wird periodisch überwacht.

Nicht Bestandteil des USZ Risk Management sind die Aufsicht des Regierungsrats und die Oberaufsicht des Kantonsrats (Aufsichtskommission Bildung und Gesundheit).

7. INFORMATION UND KOMMUNIKATION/ BERICHTERSTATTUNG

Mindestens jährlich werden die Spitaldirektion, der Finanzausschuss des Spitalrats sowie der Spitalrat selbst über das *USZ Risk Management* (inklusive IKS und Revisionen) informiert, bei ausserordentlichen Vorfällen zeitnah. Die verschiedenen Risiko- und Kontrollinstrumente verfügen über weitere Berichterstattungsinstrumente wie beispielsweise Jahres- und Qualitätsberichte zu spezifischen Themen, welche auch gesetzlich vorgegeben sein können. Eine Übersicht zur Berichterstattung je Risiko- und Kontrollinstrument ist ebenfalls im USZ Risk Management enthalten.

«Mindestens jährlich werden die Spitaldirektion, der Finanzausschuss des Spitalrats sowie der Spitalrat über das USZ Risk Management (inklusive IKS und Revisionen) informiert, bei ausserordentlichen Vorfällen zeitnah.»

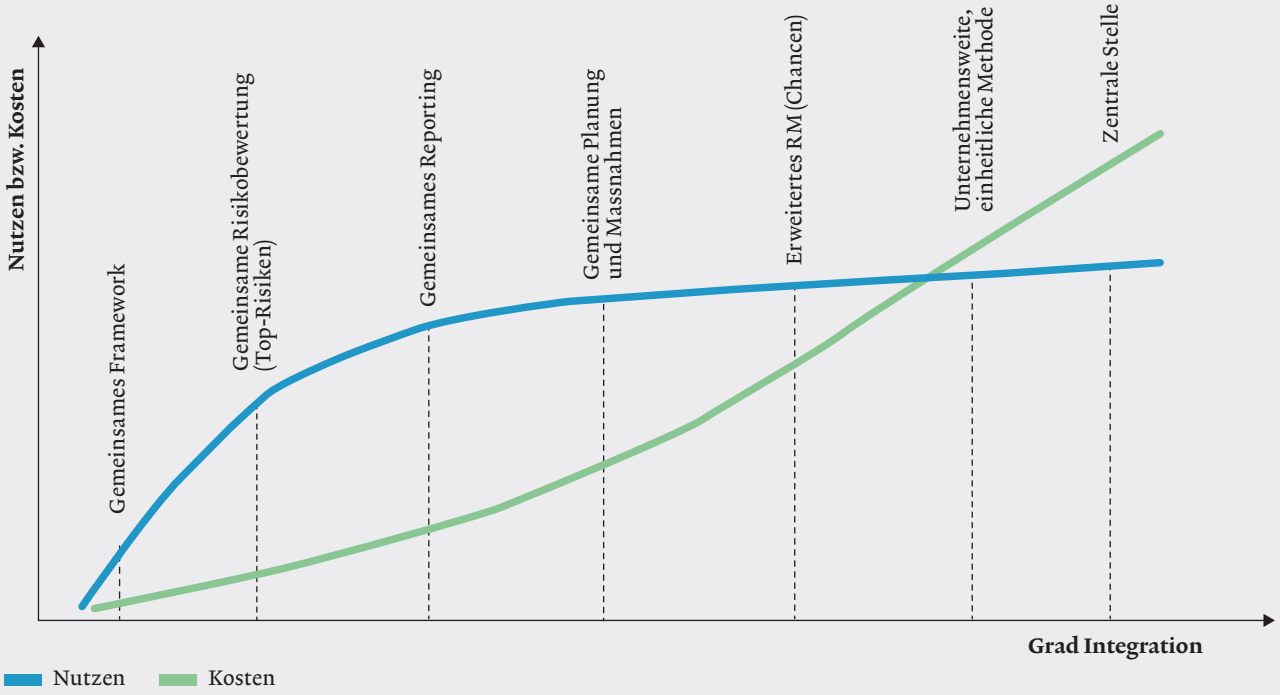
Im Jahr 2013 wurden die Verantwortlichen der verschiedenen Risikomanagement- und Kontrollfunktionen erstmals vom Finanzausschuss des Spitalrats beauftragt, die Top-Risiken aus den zuständigen Bereichen zu identifizieren und gemeinsam zu bewerten. Damit die Risiken aus den verschiedenen Themengebieten miteinander verglichen und abgestimmt werden können, wurde die herkömmliche Operationalisierung der Eintrittswahrscheinlichkeit sowie des Schadensausmasses überarbeitet; für das USZ relevante Kategorien wurden ergänzt. Im Raster «Eintrittswahrscheinlichkeit» (im Beitrag nicht abgebildet) werden die Häufigkeiten (unwahrscheinlich bis sehr wahrscheinlich) für die einzelnen Kategorien Patient, Strategie, Betriebsführung und IT unterschiedlich konkretisiert. So bedeutet «wahrscheinliches Risiko» in der Betriebsführung einmal jährlich, in der IT hingegen täglich. Im Raster «Schadensausmass» *(Abbildung 2)* werden die Einstufungen «katastrophal» bis «unbedeutend» für insgesamt acht Dimensionen durch eine Beschreibung der möglichen Folgen aufgefächert. In Workshops unterstützen die verschiedenen Kategorien zudem die Diskussion und einheitliche Bewertung von möglichen Risiken.

In einem gemeinsamen Workshop mit den Verantwortlichen der Risiko- und Kontrollinstrumente werden mindestens jährlich die Top-30-Risiken USZ mithilfe der abgestimmten und erweiterten Risikoraster für Eintrittswahrscheinlichkeit und Schadensausmass zusammengetragen und bewertet. Die Top-30-Risiken USZ sowie ein Vorschlag der Top-5-Risiken werden anschliessend der Spitaldirektion

Abbildung 2: **USZ RASTER SCHADENSAUSMASS**

	Patient	Leistungsfähigkeit	Reputation USZ Strategie, Betriebsführung	Reputation Klinik	Geschäftsergebnis	in CHF Mio.	Personenschäden	Persönliche Informationen
Unbedeutend	Vorkommnis, jedoch ohne Folgen (Critical incident, near miss)	Die Leistungsfähigkeit der Klinik bleibt unberührt	Die Reputation wird kaum beeinträchtigt. Es entstehen Umtriebe und Aufregungen	Die Reputation der Klinik wird nicht beeinträchtigt	Angesichts der Grösse der Organisation zu vernachlässigen; Budget wird kaum beeinträchtigt	bis 1	Keine oder höchstens wenige Leichtverletzte Bau: keine Verletzten	Durch Verletzung des Schutzes von Informationen entsteht Betroffenheit für ein Individuum (Ärger, Frustration), aber es geschieht kein Verstoss gegen gesetzliche oder regulative Anforderung
Gering	Minimaler Schaden; Verunsicherung des Patienten; bis drei Tage (verlängerte) Hospitalisation; Patient, Angehörige können informiert werden	Die Leistungsfähigkeit einer einzelnen Klinik bleibt unberührt; es entstehen kurzzeitige Umtriebe, Störungen im Betriebsablauf und Mehrkosten	Interesse der Medien; externer Erklärungsbedarf, aber ohne direkte und anhaltende Folgen	Die Reputation der Klinik wird nicht beeinträchtigt; es entstehen Umtriebe und Aufregungen, Verunsicherungen des Patienten, Nachfragen von Angehörigen	Schadensfolgen sind begrenzt; sie können aus dem Cashflow finanziert werden	1–5	Mehrere Verletzte Bau: keine oder wenige Leichtverletzte	Durch die Verletzung einer gesetzlichen, regulativen oder ethischen Anforderung an den Schutz von Informationen wird ein Individuum ernsthaft in Verlegenheit gebracht
Spürbar	Passagerer Schaden; leichte bis mittlere Körperverletzung ohne Dauerfolgen; mehr als drei Tage verlängerte Hospitalisation; Patient und Angehörige müssen informiert werden	Es entstehen deutliche Mehrkosten aus der Behandlung sowie aus den zusätzlichen Störungen der Prozesse	Die Reputation wird durch negative Berichte vorübergehend beeinträchtigt (Verantwortungsfragen zur Unternehmensentwicklung und lokale Medienberichterstattung)	Die Reputation der Klinik wird leicht beeinträchtigt. Es entstehen Umtriebe und Aufregungen, Nachfragen von Angehörigen; externer Erklärungsbedarf, aber ohne direkte und anhaltende Folgen	Das Jahresergebnis wird beeinträchtigt; es fällt geringer aus als geplant	5–10	Viele Verletzte, wenig Tote Bau: Mehrere verletzte Personen	Durch die Verletzung einer gesetzlichen, regulativen oder ethischen Anforderung an den Schutz von Informationen wird eine Gruppe von Individuen ernsthaft in Verlegenheit gebracht
Kritisch	Passagerer schwerer Schaden; leichte bis mittlere Körperverletzung mit Dauerfolgen ohne dauerhafte Pflegebedürftigkeit	Die Leistungsfähigkeit für einzelne Kliniken wird beeinträchtigt	Die Reputation wird regional über längere Zeit geschädigt; Verantwortungsfragen zur Unternehmensentwicklung und negative Medienberichte	Die Reputation der Klinik wird durch negative Berichte, Strafanzeigen, Untersuchungen und lokale Medienberichterstattung beeinträchtigt	Das Jahresergebnis wird nachhaltig beeinflusst und durch das Risiko weitgehend verzehrt	10–20	Viele Schwerverletzte, mehrere Tote Bau: Schwer verletzte Personen	Durch die Verletzung einer gesetzlichen, regulativen oder ethischen Anforderung an den Schutz von Informationen gelangen vollständige Patienteninformationen in den Schwarzmarkt (Dark Net) und werden zum Verkauf angeboten
Katastrophal	Dauerschaden schwer; schwere Körperverletzung mit Dauerfolgen und dauerhafter Pflegebedürftigkeit; Tod des Patienten	Die Fortführung des bisherigen Leistungsspektrums ist bedroht; Leistungsangebot muss vorübergehend angepasst werden	Die Reputation wird überregional, irreparabel geschädigt; Verantwortungsfragen zur Unternehmensentwicklung und negative Medienberichte	Die Reputation wird überregional, schwer reparabel geschädigt, z. B. durch Strafanzeigen und negative Berichterstattung	Das Eigenkapital wird angegriffen; es muss eine zusätzliche Fremdfinanzierung beschafft werden	> 20	Sehr viele Schwerverletzte, über 10 Tote Bau: Schwerverletzte, Tote	Durch die Verletzung einer gesetzlichen, regulativen oder ethischen Anforderung an den Schutz von Informationen gelangen massenhaft besonders schützenswerte Informationen an die Öffentlichkeit

Abbildung 3: **KOSTEN UND NUTZEN BEI ZUNEHMENDER INTEGRATION**



berichtet. Die Spitaldirektion setzt sich mit den Risiken auseinander und definiert aus ihrer Sicht die Top-5-Risiken USZ. Selbstverständlich ist die Spitaldirektion frei, Risiken anders zu beurteilen oder neue Risiken hinzuzufügen.

Zusätzlich werden die im abgelaufenen Geschäftsjahr effektiv eingetretenen Risiken und Gefahren je Risiko- und Kontrollinstrument aufgenommen und in einem Bericht zusammengefasst.

Die aktualisierte Übersicht Risikomanagement und IKS USZ, die Top-30- und Top-5-Risiken sowie die eingetretenen Risiken/Gefahren im abgelaufenen Geschäftsjahr werden im Anschluss der Spitaldirektion und dem Spitalrat in drei Dokumenten kommuniziert:

1. *Konzept:* Übersicht Konzept Risikomanagement und IKS am USZ (jährlich aktualisiert);
2. *Top-Risiken:* Top-30-Risiken USZ und Top-5-Risiken aus Sicht Spitaldirektion;
3. *Eingetretene Risiken:* Eingetretene Risiken/Gefahren im abgelaufenen Geschäftsjahr je Risiko- und Kontrollinstrument.

8. FAZIT

Die Übersicht «Konzept Risikomanagement und Internes Kontrollsystem am USZ» dient der Spitaldirektion, dem Spitalrat und dem Finanzausschuss des Spitalrats als Übersicht sowie Grundlage für die weitere Planung und Definition von Massnahmen.

Das *USZ Risk Management* ist eine an COSO ERM sowie «3-Lines-of-Defense» angelehnte, übersichtliche und systematische «Architektur» der vorhandenen Kontroll- und Überwachungsinstrumente, entspricht aber nicht einem unternehmensweiten integrierten Risikomanagement. Die verschiedenen Instrumente sind vielmehr spezifisch für ihren Verwendungszweck konzipiert und werden weitgehend unabhängig voneinander betrieben. Es handelt sich oft auch um Branchenstandards.

Wie in der Ausgangslage festgehalten wurde, beurteilt das USZ zum heutigen Zeitpunkt ein unternehmensweites integriertes Risikomanagement mit einer einheitlichen Methode oder beispielsweise einer zentralen Stelle als nicht zweckmässig und mit einem negativen Nutzen-Kosten-Verhältnis (so auch schematisch in *Abbildung 3* dargestellt). Bereits für

> *«Wichtig ist, dass Risiken auf allen Stufen identifiziert, beurteilt sowie bewirtschaftet und die Verantwortungen wahrgenommen werden.»*

den Aufbau eines integrierten Risikomanagements ist mit einem enormen internen und externen Ressourcenbedarf zu rechnen. Der Breite der verschiedenen Risiken werden die unterschiedlich eingesetzten Methoden besser gerecht. Im jeweiligen Fachgebiet verwendete Methoden können auch besser miteinander verglichen werden, und zusätzlich muss kein Instrument auf die bisher verwendete Methode verzichten oder für die identifizierten Risiken umfangreiche Überleitungen vornehmen, um diese mit anderen zu vergleichen. Hingegen bietet das USZ Risk Management die gemeinsame Grundlage für die Entdeckung allfälliger Kontrolllücken sowie für eine einheitliche Beurteilung der Risiken und für die Berichterstattung.

Das vorhandene Konzept kann bei Bedarf ohne grossen Ressourcenaufwand angepasst oder weiterentwickelt werden. Im Jahr 2017 wurde zum Beispiel den ISO-zertifizierten Kliniken und Instituten des USZ eine auf das USZ Risk Management abgestimmte Vorlage zur Beurteilung und Dokumentation der Risiken zur Verfügung gestellt. Mögliche Anpassungen und Weiterentwicklungen bestehen zudem in den nachfolgenden Themen:
→ Identifikation und Bewirtschaftung nicht nur von Risiken im engeren Sinn, sondern auch von Chancen; → Ableitung gemeinsamer Massnahmen durch verschiedene Risiko- und Kontrollinstrumente für definierte Schwerpunkte des USZ Risk Management; → Optimierung des Informationsaustauschs.

Mit dem vorhandenen Risikomanagementsystem konnten die gesetzten Ziele mit einem geringen Ressourcenaufwand umgesetzt werden. Wichtig ist, dass Risiken auf allen Stufen identifiziert, beurteilt sowie bewirtschaftet und die Verantwortungen wahrgenommen werden. Das System soll regelmässig kritisch beurteilt, mögliche Optimierungs- und Harmonisierungsmassnahmen aufgezeigt und umgesetzt werden. ■

Anmerkungen: 1) COSO – Committee of Sponsoring Organizations of the Treadway Commission: Internal Control – Integrated Framework. Jersey City 1992; COSO – Committee of Sponsoring Organizations of the Treadway Commission: Enterprise Risk Management – Integrated Framework. Jersey City 2004. **2)** Committee of Sponsoring Organizations of the Treadway Commission: Internal Control – Integrated Framework. Framework and Appendices. Jersey City 2013; COSO – Committee of Sponsoring Organizations of the Treadway Commission: Internal Control – Integrated Framework. Internal Control over External Financial Reporting: A Compendium of Approaches and Examples. Jersey City 2013; COSO – Committee of Sponsoring Organizations of the Treadway Commission: Internal Control – Integrated Framework. Illustrative Tools for Assessing Effectiveness of a System of Internal Control, Jersey City 2013. **3)** COSO – Committee of Sponsoring Organizations of the Treadway Commission: Enterprise Risk Management – Integrated Framework. Jersey City 2004. **4)** European Confederation of Institutes of Internal Auditing (ECIIA)/Federation of European Risk Management Associations (FERMA): Guidance on the 8th EU Company Law Directive. Article 41, September 2010; Institute of Internal Auditors (IIA): Three Lines of Defence in Effective Risk Management and Control, Position Paper, January 2013. **5)** Pfaff, D./Ruud, F.: Schweizer Leitfaden zum Internen Kontrollsystem (IKS), 7. Aufl., Zürich 2016, S. 29.